NYS SkillsUSA Standards

INTERNETWORKING

PURPOSE

To evaluate each competitor's preparation for employment and to recognize outstanding students for excellence and professionalism in the field of internetworking.

ELIGIBILITY

Open to active NYS SkillsUSA members currently enrolled in programs with internetworking as an occupational objective. Each state may send one high school competitor.

CLOTHING REQUIREMENTS

NYS SkillsUSA Business Professional

- White polo shirt (plain or with SkillsUSA or SkillsUSA NY monogram) or White dress shirt with
- plain black tie with no pattern or a SkillsUSA black tie, or business like white collarless blouse or white blouse with small plain collar.
- Black dress slacks (accompanied by black dress socks or black or skin-tone seamless hose) or black dress skirt (knee-length, accompanied by black or skin-tone seamless hose).
- Black leather shoes that are not backless or open toe

Note: **Contestants must wear their contest clothing to the contest orientation meeting. Also bring #2 pencil, resume, safety assurance form and conference program.**

EQUIPMENT AND MATERIALS

1. Supplied by the NYS chair/committee:
    a. Tables and chairs for the written portion of the contest
2. Supplied by contestant:
    a. Laptop computer with wireless, Ethernet connection and COM port (USB with adapter)
    b. Contestants' computers must be pre-loaded with the most current version of CISCO student version. (not instructor version)
    c. All competitors must create a one-page resume. See "Resume Requirement" below for guidelines.

RESUME REQUIREMENT

Competitors must create a one-page resume to submit at orientation.

DEVICES

Cell phones or other electronic devices not approved by the NYS Chairperson will be collected by the contest chair during the competition. Chairpersons will announce their acceptance by listing it on their standard or at the orientation meeting. In case of emergencies advisors should allow the competitors to take their phones to the contest areas.

If the competitor uses their device in a manner which compromises the integrity of the competition, the competitor's score may be penalized.

SCOPE OF THE COMPETITION

The competition is defined by current industry technical standards and will consist of five parts: An end-to-end network configuration, a troubleshooting exercise, a simulation TAC call, a written exam, and a design project.

KNOWLEDGE PERFORMANCE

All competitors are required to take the SkillsUSA professional development test online.

The competition will include a written exam assessing knowledge of general networking concepts.

SKILL PERFORMANCE

The competition may include but is not limited to the following assessments.

Design problem
Competitors will be evaluated on their ability to design a network that meets specific requirements. If a network design problem is in use this year it will be posted on the Facebook page and via the SkillsUSA Internetworking Competition page in Remind by the Thursday prior to the competition's start.

End-To-End Networking
Given a set of networking equipment (cable, fiber, hubs/switches routers, etc.) the student must, in a finite amount of time, install or repair a network and demonstrate that the installation properly runs internet applications.

Given a logical topology and network requirements, the students will be able to develop a usable network that meets or exceeds the documentation provided. The vision and context are that client companies would request a demonstration booth that runs a particular internet application, and the student, given equipment and tools, would provide the appropriate connectivity for the application to run successfully.

Technical Assistance Call
The student must solve a networking problem while on the phone with a customer. This is a simulation of working in a Technical Assistance Center. This station not only assesses technical skill, but also communication and customer service.

Written Exam
The student must answer questions related to CCNA-level networking.

Troubleshooting
Competitors will be evaluated on their ability to troubleshoot and correct issues in an already existing network.

Wireshark Analysis
Competitors will be evaluated on their ability to capture and analyze network traffic utilizing Wireshark.

ADDITIONAL INFORMATION AND COMPETITION UPDATES

- For any competition updates, please reference the NYS SkillsUSA web site nysskillsusa.org.
- It is crucial to check the NYS SkillsUSA website, as we may use it to post work, we expect competitors to have completed prior to their arrival at the national competition.

STANDARDS AND COMPETENCIES

WORK 1.0 — Network Fundamentals

1.1. Explain the role and function of network components
- 1.1.1. Routers
- 1.1.2. L2 and L3 switches
- 1.1.3. Next-generation firewalls and IPS
- 1.1.4. Access points
- 1.1.5. Controllers (Cisco DNA Center and WLC)
- 1.1.6. Endpoints
- 1.1.7. Servers
- 1.1.8. PoE

1.2. Describe characteristics of network topology architectures
- 1.2.1. 2 tier
- 1.2.2. 3 tier
- 1.2.3. Spine-leaf
- 1.2.4. WAN
- 1.2.5. Small office/home office (SOHO)
- 1.2.6. On-premises and cloud

1.3. Compare physical interface and cabling types
- 1.3.1. Single-mode fiber, multimode fiber, copper
- 1.3.2. Connections (Ethernet shared media and point-to-point)
- 1.3.3. Concepts of PoE

1.4. Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed)

1.5. Compare TCP to UDP

1.6. Configure and verify IPv4 addressing and subnetting

1.7. Describe the need for private IPv4 addressing

1.8. Configure and verify IPv6 addressing and prefix

1.9. Compare IPv6 address types
- 1.9.1. Global unicast
- 1.9.2. Unique local
- 1.9.3. Link local
- 1.9.4. Anycast
- 1.9.5. Multicast
- 1.9.6. Modified EUI 64

1.10. Verify IP parameters for Client OS (Windows, Mac OS, Linux)

1.11. Describe wireless principles
- 1.11.1. Nonoverlapping Wi-Fi channels
- 1.11.2. SSID

1.11.3. RF
1.11.4. Encryption
1.12. Explain virtualization fundamentals (virtual machines)
1.13. 1.13 Describe switching concepts
1.13.1. MAC learning and aging
1.13.2. Frame switching
1.13.3. Frame flooding
1.13.4. MAC address table

WORK 2.0 — Network Access

2.1. Configure and verify VLANs (normal range) spanning multiple switches
2.1.1. Access ports (data and voice)
2.1.2. Default VLAN
2.1.3. Connectivity
2.2. Configure and verify interswitch connectivity
2.2.1. Trunk ports
2.2.2. 802.1Q
2.2.3. Native VLAN
2.3. Configure and verify Layer 2 discovery protocols (Cisco Discovery Protocol and LLDP)
2.4. Configure and verify (Layer 2/Layer 3) EtherChannel (LACP)
2.5. Describe the need for and basic operations of Rapid PVST+ Spanning Tree Protocol and identify basic operations
2.5.1. Root port, root bridge (primary/secondary), and other port names
2.5.2. Port states (forwarding/blocking)
2.5.3. PortFast benefits
2.6. Compare Cisco Wireless Architectures and AP modes
2.7. Describe physical infrastructure connections of WLAN components (AP,WLC, access/trunk ports, and LAG)
2.8. Describe AP and WLC management access connections (Telnet, SSH, HTTP,HTTPS, console, and TACACS+/RADIUS)
2.9. Configure the components of a wireless LAN access for client connectivity using GUI only such as WLAN creation, security settings, QoS profiles, and advanced WLAN settings

WORK 3.0 — IP Connectivity

3.1. Interpret the components of routing table
3.1.1. Routing protocol code
3.1.2. Prefix
3.1.3. Network mask
3.1.4. Next hop
3.1.5. Administrative distance
3.1.6. Metric
3.1.7. Gateway of last resort
3.2. Determine how a router makes a forwarding decision by default
3.2.1. Longest match
3.2.2. Administrative distance
3.2.3. Routing protocol metric

3.3. Configure and verify IPv4 and IPv6 static routing
    3.3.1. Default route
    3.3.2. Network route
    3.3.3. Host route
    3.3.4. Floating static
3.4. Configure and verify single area OSPFv2
    3.4.1. Neighbor adjacencies
    3.4.2. Point-to-point
    3.4.3. Broadcast (DR/BDR selection)
    3.4.4. Router ID
3.5. Describe the purpose of first hop redundancy protocol

WORK 4.0 — IP Services

4.1. Configure and verify inside source NAT using static and pools
4.2. Configure and verify NTP operating in a client and server mode
4.3. Explain the role of DHCP and DNS within the network
4.4. Explain the function of SNMP in network operations
4.5. Describe the use of syslog features including facilities and levels
4.6. Configure and verify DHCP client and relay
4.7. Explain the forwarding per-hop behavior (PHB) for QoS such as classification, marking, queuing, congestion, policing, shaping
4.8. Configure network devices for remote access using SSH
4.9. Describe the capabilities and function of TFTP/FTP in the network

WORK 5.0 — Security Fundamentals

5.1. Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)
5.2. Describe security program elements (user awareness, training, and physical access control)
5.3. Configure device access control using local passwords
5.4. Describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)
5.5. Describe remote access and site-to-site VPNs
5.6. Configure and verify access control lists
5.7. Configure Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)
5.8. Differentiate authentication, authorization, and accounting concepts
5.9. Describe wireless security protocols (WPA, WPA2, and WPA3)
5.10. Configure WLAN using WPA2 PSK using the GUI

WORK 6.0 — Automation and Programmability

6.1. Explain how automation impacts network management
6.2. Compare traditional networks with controller-based networking
6.3. Describe controller-based and software defined architectures (overlay, underlay, and fabric)
    6.3.1. Separation of control plane and data plane
    6.3.2. North-bound and south-bound APIs

6.4. Compare traditional campus device management with Cisco DNA Center enabled device management
6.5. Describe characteristics of REST-based APIs (CRUD, HTTP verbs, and data encoding)
6.6. Recognize the capabilities of configuration management mechanisms Puppet, Chef, and Ansible
6.7. Interpret JSON encoded data

WORK 7.0 — Important Topics Outside the CCNA's Scope

7.1. Configure and troubleshoot the following Routing Protocols
  7.1.1. RIP (v1 and 2)
  7.1.2. OSPFv2
  7.1.3. EIGRP
  7.1.4. BGP
  7.1.5. Static Routing
7.2. Configure and Troubleshoot Spanning-Tree Protocol (Rapid and regular)
7.3. Configure and Troubleshoot VLAN Trunking
7.4. Configure and Troubleshoot Windows System administration
  7.4.1. DNS
  7.4.2. Active Directory Users, Computers, and Groups
  7.4.3. DHCP
  7.4.4. NTP
  7.4.5. IP Settings
7.5. Configure and Troubleshoot Linux System administration
  7.5.1. DNS
  7.5.2. Users and Groups
  7.5.3. DHCP
  7.5.4. NTP
  7.5.5. IP Settings
  7.5.6. Services
7.6. Perform Password Recovery on Network Devices
7.7. Explain L2 and L3 headers
7.8. Collect and Interpret packet captures